Classical programmability is enough for quantum circuits universality in approximate sense

Alexander Yu. Vlasov

FRC/IRH, 197101 Mira Street 8, St.–Petersburg, Russia

***

It was shown by M. A. Nielsen and I. L Chuang [1], that it is impossible to build *strictly* universal programmable quantum gate array, that could perform any unitary operation *precisely* and it was suggested to use probabilistic gate arrays instead. In present work is shown, that if to use more physical and weak condition of universality (suggested already in earliest work by D. Deutsch [3]) and to talk about simulation with arbitrary, but finite precision, then it is possible to build universal programmable gate array. But now the same no-go theorem by Nielsen and Chuang [1] will have new interesting consequence — controlling programs for the gate arrays can be considered as pure classical. More detailed design of such deterministic quantum gate arrays universal "in approximate sense" is considered in the paper.

1   Introduction

In the paper [1] was discussed conception of programmable quantum gate arrays, i.e., some quantum circuits are acting on a system in form $|d; P\rangle \equiv |d\rangle \otimes |P\rangle$ considered as *data register* $|d\rangle$ and *program register* (or simply *program*) $|P\rangle$. Similar with conception of usual classical computer, it was considered, that circuit acts as some fixed unitary transformation U on whole system and different transformations U_P of data related only with content P of program register, i.e:

$$\mathsf{U}\big(|d\rangle \otimes |P\rangle\big) = (U_P|d\rangle) \otimes |P'\rangle. \tag{1}$$

It should be emphasized, here U_P is same for any state of data register $|d\rangle$ i.e., depends only on program $|P\rangle$, and states of these two registers are not entangled before and after application of U.

In relation with such a definition in [1] was noticed, that if to write the Eq. (1) for two different programs $|P\rangle$ and $|Q\rangle$ and corresponding unitary data transformations $|U_P\rangle$ and $|U_Q\rangle$, it is simple to find by considering scalar products

of both parts, that if $U_P \neq \phi U_Q$ for some complex number ϕ then the states of program register must be orthogonal for different programs:

$$\langle P \mid Q \rangle = 0. \tag{2}$$

The property Eq. (2) treated in [1] as demonstration that "... no universal quantum gate array (of finite extent) can be realized. More specifically, we show that every implementable unitary operation requires an extra Hilbert space dimension in the program register." Due to such a problem in the article [1] was suggested idea of (exactly) universal stochastic programmable gate array developed further by other authors [10].

It was no-go theorem for "universality in exact sense" [2], but fortunately already in initial definition of universal quantum computer [3] was shown possibility of using some discrete everywhere dense subset in the whole continuous space of unitary operators, it is called sometime "universality in approximate sense" [2].

Here is shown, that in the approximate sense such universal programmable quantum gate arrays with *possibility of approximation of any unitary transformation of data register with given precision* are really exist and constructions are quite simple and may be described directly. But the property Eq. (2) is again very important, because if all different possible states of program register are orthogonal, it is possible without lost of generality to find implementation of same array with all different programs are elements of computational basis and superpositions of the states for the program register are *never used* and so any such array can be designed with possibility of using only classical programs. It is shown and discussed with more extent in relation with particular design used below.

2 Universal programmable quantum gate arrays

It is more convenient here to use notation with program register first, i.e., $|P; d\rangle$ instead of $|d; P\rangle$. The reason is more simple form of operations like *CONTROL-U*:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}. \tag{3}$$

Such operator acts on second qubit as U only if first qubit is $|1\rangle$, but $|0\rangle$ does not change anything. A straightforward generalization for arbitrary $N \times N$ matrix U and one program qubit is $2N \times 2N$ matrix:

$$\begin{pmatrix} 1 & 0 \\ 0 & U \end{pmatrix}, \tag{4}$$

where 1 and 0 are $N \times N$ unit and zero matrices.

Let us now consider simple programmable gate array with dimension of program is M and data register is N. For quantum computation with qubits $M = 2^m$ and $N = 2^n$. Let us introduce a matrix (cf. [5]) $\mathsf{S} = \mathsf{S}_{\{U_1,\ldots,U_M\}}$:

$$\mathsf{S} = \begin{pmatrix} U_1 & & & \text{\Large 0} \\ & U_2 & & \\ & & \ddots & \\ \text{\Large 0} & & & U_M \end{pmatrix}. \tag{5}$$

where $U_1, \ldots, U_M$ are M matrices $N \times N$. It is clear, that such $NM \times NM$ matrix $\mathsf{S} = \mathsf{S}_{\{U_1,\ldots,U_M\}}$ acts as:

$$\mathsf{S}\big(|P\rangle \otimes |d\rangle\big) = |P\rangle \otimes (U_P|d\rangle). \tag{6}$$

and it corresponds to Eq. (1) with $P = P'$ is simply number of matrix U_P.

Such matrix was suggested for description of conditional quantum dynamics in [5], but Eq. (2) introduced in [1] and discussed here shows also, that we do not need more general control with superpositions of basis states of program (control register).

Let us consider a case with $\{U_1, \ldots, U_M\}$ are universal set of gates (in approximate sense) for some quantum circuits with n qubits together with unit matrix $U_0 \equiv \mathbf{1}$. Here $N = 2^n$ and for design with matrix S size of program is small enough — number of qubits in the register is $m = \lceil \log_2 M \rceil$. But if due to technical problem with implementation we should use set of $CONTROL\text{-}U_i$ gates Eq. (4) instead of S Eq. (5), then number of program qubits are $m = M$.

We may use small universal sets with only one and two-qubit gates [2, 7, 8, 9]. For example, if to choose a set with $n + 2$ one-qubit gates and $n - 1$ two-gates acting on pairs of neighboring qubits from [9] together with unit matrix, then number of qubit in control register is $m = \lceil \log_2(2n + 2) \rceil$ in best case and even in worst case discussed earlier it is $2n + 2$.

Let us now extend program register up to km qubits, i.e. state of arrays described now as $|P_k; \ldots; P_2; P_1; d\rangle$ and together with matrix S acting only on last $m + n$ qubits $|P_1; d\rangle$ as described above let us consider unitary matrix R acting on program register as *right cyclic shift*:

$$\mathsf{R}\,|P_k; \ldots; P_2; P_1; d\rangle = |P_1; P_k; \ldots; P_2; d\rangle \tag{7}$$

It is clear, that if $\mathsf{U} = \mathsf{RS}$, then operator U^k can perform with data arbitrary sequence of up to k operators $\{U_1, \ldots, U_M\}$:

$$\mathsf{U}^k\big(|0; \ldots; 0; P_l; \ldots; P_1\rangle \otimes |d\rangle\big) = |0; \ldots; 0; P_l; \ldots; P_1\rangle \otimes (U_{P_l} \cdots U_{P_1}|d\rangle) \tag{8}$$

here U_0 is unit operator used to fill out $k - l$ positions for $l < k$ and $U_{P_l} \cdots U_{P_1} \cong U$ is arbitrary product of gates from the finite universal set $\{U_1, \ldots, U_M\}$ for approximation of any data gate U with necessary precision. Usually number of terms in product $l \gg M$. If minimal error of simulation is given, it is possible to

find necessary number k and then U^k is universal circuit with bounded chosen accuracy.

The idle $k - l$ steps make more clear advantage of a design well known in classical theory of computations — instead of consideration of whole circuit U^k it is possible to introduce notion of *one computational step* U. In such approach action of quantum circuit similar with usual CPU "timing" with repeating of same U till halting.

It is also useful, then due to algorithm of approximation we need to apply same loop many times, for example instead of some operator U may be used "j-th root" $U^{1/j}$ [6, 9] and the circuit should be applied j times and can be expressed as $\mathsf{U}^{k\,j}$.

Here were examples of some general architecture for programmable quantum gate arrays — we have n data qubits and program with $p + m$ qubits of two different kinds. Here are m control qubits of quantum controller together with n data qubits form input for "quantum step operator" S described by Eq. (5).

Generalization of R operator is not necessary simple rotation, because such model may use too many space. The R is equivalent of reversible classical[1] circuit acting on $p + m$ (qu)bit program register with purpose to generate necessary index of universal quantum gate for quantum controller during simulation.

It should be mentioned also yet another advantage and special property of "pseudo-classical", i.e., orthogonal states of program register. Only for such kind of programs it is possible to make measurements of state without destruction and so use tools like *halt* bit. It is also further justification of notion of *variable lenght* algorithms already used above.

The consideration shows possible model of programmable "quantum chip". It has three different kinds of "wiring": quantum, intermediate and classical "buses" with d, m and p (qu)bits respectively and two different kinds of circuits: quantum controller acting on quantum bus and controlled by intermediate bus and reversible classical (or Qu-ERCC) circuit with input via classical bus for control of intermediate bus.

Due to result about orthogonality of programs [1] the design is general for deterministic circuits with pure states, and does not need some special quantum control, i.e, superpositions in program register, only data is necessary quantum.

On the other hand, for circuits with mixed states, stochastic programmable quantum arrays [1, 10] control already is not limited by the (pseudo) classical case discussed here.

References

[1] M. A. Nielsen and I. L Chuang, "Programmable quantum gate arrays," Phys. Rev. Lett. **79** 321–324, (1997).

---

[1] "Qu-ERCC" — Quantum Equivalent of Reversible Classical Circuit, or simply "classical gate" in terminology used by [6]

[2] R. Cleve, "An introduction to quantum complexity theory," *Preprint* `quant-ph/9906111`, (1999).

[3] D. Deutsch, "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer," Proc. R. Soc. London **A 400**, 97–117 (1985).

[4] D. Deutsch, "Quantum Computational Networks," Proc. R. Soc. London **A 425**, 73–90 (1989).

[5] A. Barenco, D. Deutsch, A. K. Ekert, and R. Jozsa, "Conditional quantum dynamics and logic gates," Phys. Rev. Lett. **74**, 20, 4083–4086 (1995).

[6] D. Deutsch, A. Barenco, and A. Ekert, "Universality in quantum computation," Proc. R. Soc. London **A 449**, 669 (1995).

[7] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. W. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," Phys. Rev. A **52**, 5, 3457–3467 (1995);

[8] D. P. DiVincenzo, "Two-bit gates are universal for quantum computation," Phys. Rev. A **51**, 1015 – 1022 (1995).

[9] A. Yu. Vlasov, "Clifford algebras and universal sets of quantum gates," E-print: `quant-ph/0010071` (2000) [accepted for publication in Phys. Rev. A (2001)].

[10] G. Vidal, L. Masanes, and J. I. Cirac, "Storing quantum dynamics in quantum states: stochastic programmable gate for $U(1)$ operations," *Preprint* `quant-ph/0102037`, (2001).